(U//FOUO) WINDSTOP/2P
System Highlights



MUSCULAR

- Minor circuit move, not collection suite move (so-2013-00762)
- XKS FP updates across TU systems / NArchive throttle update



INCENSER

- INCS4 config issue (uo-2013-00471)

Speaker's Notes

From Feb 28 2013: Proposed/imminent latest DO/Volume reduction: Narchive

BLUF: Requested S2 concurrence at S2 TLC on 25 Feb with partial throttling of content from Yahoo, Narchive email traffic which contains data older than 6 months from MUSCULAR. Numerous S2 analysts have complained of its existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4th of the total daily collect).

Background: Since July of 2012, Yahoo has been transferring entire email accounts using the Narchive data format (a proprietary format for which NSA had to develop custom demultiplexers). To date, we are unsure why these accounts are being transferred – movement of individuals, backup of data from overseas servers to US servers, or some other reason. There is no way currently to predict if an account will be transferred via Yahoo Narchive.

Currently, Narchive traffic is collected and forwarded to NSA for memorialization in any quantity only from DS-200B. On any given day, Narchive traffic represents 25% (15GB) of DS-200B's daily PINWALE content allocation (60GB currently). DS-200B is scheduled to be upgraded in the summer of 2013; it is likely that memorialized Narchive traffic, if still present in the environment, will grow proportionally (i.e. double now, to 30 GB/day).

Narchive traffic is mailbox formatted email, meaning unlike Yahoo webmail, any attachments present would be collected as part of the message. This is a distinct advantage. However, it has not been determined what causes an Narchive transfer of an account, so these messages are rarely collected "live".

Based on analysis of Narchive email data by [redacted] and [redacted], we were able to indentify statistics for the original communications date for Narchive email messages collected:

< 30 days	1118	11%
> 30 days, < 90 days	1758	17%
> 90 days < 180 days	1302	13%
> 180 days, < 1 year	2592	26%
> 1years, < 5 years	3084	31%
> 5years	154	>1%

Numerous target offices have complained about this collection "diluting" their workflow. One argument for keeping it is that it provides a retrospective look at target activity – this argument is hampered by a) the unreliable and non-understood nature of when the transfer occurs for an account, and b) that FISA restrospective collection would retrieve the exact same data "on demand".

SSO Optimization believes that while this is "valid" collection of content, the sheer volume and the age – coupled with the unpredictable nature of Narchive activity – makes collecting older data a less desirable use of valuable resources. 59% of Narchive email collected was originally sent and received more than 180 days after collection. This represents about 8.9 GB a day of "less desirable" collection – long term allocation that could be easily filled with more timely, useful FI from this lucrative SSO site. As always with our optimization, the data would still be available at the site store for SIGDEV. This would not impact metadata extraction.

Past DO volume reduction efforts:
Webmail OAB- Leap day 2012: the original defeat only targeted gmail, yahoo, and hotmail webmail protocol
FB buddylist sampling since last year

Today: FB OAB defeat/atxks/facebook/ownerless_addressbook : this is a JSON addressbook